**IT Applications, Ch 7, Information Management**

Threats to the integrity and security of data and information stored, communicated and disposed of by organisations.

Complete the following from p 270-

**Deliberate threats**

1. When does intentional damage occur?  
   Occurs when an individual or a group deliberately sets out to cause problems within an information system. Their aim may be to damage the hardware or alter the data in some way.
2. Unauthorised access is both physical and logical. Explain what this means?
3. Computer Virus
   1. Describe the nature of this virus.  
      The computer virus, so named because it infects a machine in much the same manner as a biological virus might infect a human, is one of the most common and easily transmitted threats to data stored on computer.
   2. What is the main purpose of a virus?  
      A virus is designed to affect the running of a PC in a manner unintended by the user.
   3. What is meant by the term, payload?  
      The payload is the action that the Virus is designed to carry out. Eg. Delete files from the hard disk, etc.
   4. Describe a worm?  
      They attach themselves to an email then locate all email addresses in the victims email program and then it sends the infected message to all of the email addresses.
   5. List the other types of viruses, p 272, fig. 7-10.  
      Boot infectors, executable, macro, time bomb, logic bomb, worm, Trojan horse, resident and polymorphic.
   6. How do viruses mainly spread?  
      The most common is through an email file attachment, or by the transfer of infected files on a removable storage device. Another, less common source of infection is by different users accessing an infected file on a network.
4. Hacking/Cracking
   1. Who is a hacker and what damage do they cause?  
      A hacker is a person who gains unauthorised access to an information system through logical means in order to look at the stored data or simply for the challenge.  
      Most commonly associated with breaking into information systems and looking at any interesting or confidential material that they may contain.
5. Tampering with files
   1. Describe how employees tamper with files.  
      in some cases, employees have tampered with salary amounts and even erased important medical files from hospital databases or patient details. In other cases, research finding have been alter to suit particular stakeholders.
   2. What is industrial sabotage?  
      there is even the possibility of countries hostile to a nuclear weapon-equipped power, committing industrial sabotage by changing security codes to gain control of the devices.
6. Information theft
   1. Why does this occur?  
      All organisations look for an edge over their competitors. In some cases, less scrupulous businesses may resort to stealing information from other companies.
7. Vandalism of hardware
8. Theft of hardware

**Accidental threats**

1. User error
   1. List some common examples of user error.  
      Copying an older version of a file over a newer version or formatting a disk that contains important data.
   2. What processes are in place to limit user error.  
      Many programs try to limit the amount of data lost by users by building in safeguards such as dialogue boxes to confirm particular actions. Most application will ask if a user wishes to save changes to a document before closing it and will request confirmation before sending a document to the recycle or trash bin and removing it complete from the system.
2. Failure to follow file-management procedures
   1. List common errors of employees in saving files.  
      Often, employees may believe that they have lsot important files for one of three reasons:
      * File extensions have been left off
      * Non-descriptive filenames were used
      * Folder were improperly used.

**Technical Failure**

1. List some examples of technical failure.  
   there are several key causes of accidental hardware damage. Some of these are due to technical failure, such as breakage, while others are event based, such as variation in electricity flow, smoke, fire and water damage.

**Consequences of violating security and privacy measures, p 278**

1 List three important consequences if security measures are violated.  
 These consequences include, but are not limited to:  
 - Breaches of privacy

- Loss of intellectual property

- Loss of income due to unavailability of information or services.